UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF	)	
ACCOUNT INFORMATION ASSOCIATED	)	
WITH KIK USERNAME "Evangeliant"	)	
THAT IS STORED AT PREMISES	)	
CONTROLLED BY MEDIALAB, INC.	)	**Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, S. Vincent M. Chambers, a Special Agent with the Department of Justice, Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application for a search warrant for content and records associated with a certain Kik user account that is stored at premises owned, maintained, controlled, or operated by MediaLab, Inc., a social networking company headquartered in Santa Monica, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require MediaLab to disclose to the government records and other information in its possession (including the content of communications) pertaining to the Kik account associated with the username "evangeliant" (hereinafter referred to as the "SUBJECT ACCOUNT"), which is stored at the premises owned, maintained, controlled, or operated by MediaLab, Inc. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

AGENT BACKGROUND

2. I am a Special Agent of the FBI. I entered on duty as a Special Agent of the FBI on September 27, 2004. I was assigned to the Boston Division of the FBI upon graduation from New Agent Training at Quantico, Virginia in January 2005. Immediately after my January 2005 graduation, I was assigned to FBIHQ from January 2005 until May 2005 conducting Presidential background investigations on

candidates being placed into positions of trust in the executive branch of the US government. I completed DEA Basic narcotics training in 2005 and investigated drug and gang violations for over eight years. In 2013 I was sent on temporary assignment to Haiti to investigate violations of the Foreign Corrupt Practices Act (FCPA). Upon my return to the Boston Division I was assigned to a White-Collar Crime Squad and continued my investigation into FCPA violations. In December 2015, I was promoted to Supervisory Special Agent and returned to FBIHQ. While at FBIHQ, from December 2015 until June 2017, I program managed counter-narcotics efforts from Maine to Virginia and San Juan, Puerto Rico. In June 2017 I returned to the Boston Division of the FBI and was assigned to the Lowell Resident Agency (RA) as the Principle relief Agent and was placed in charge of the Lowell RA's Transnational Organized Crime Western Hemisphere Task Force (TOC WEST TF). I was the case agent on several narcotics investigations which utilized sophisticated investigation techniques such as undercover operations. In February 2018 I was transferred to the Bedford, New Hampshire RA of the Boston Division. From February 2018 until August 2021 I was assigned to the New Hampshire Safe Streets Gang Task Force (NHSSGTF). In April of 2019, I became the Team Leader of the NHSSGTF. In August 2021, I stepped down as the Team Leader of the NHSSGTF and currently conduct investigations involving white-collar crime, crimes against children and cybercrime. I am currently enrolled in Boston College's Cybersecurity and Governance master's degree program. I earned a bachelor's degree from Norwich University, Military College of Vermont, in International Relations, with a minor in French and a minor in English. From May 1994 until May 2004, I was a Commissioned Regular Army Officer and attained the rank of Captain before joining the FBI.

3. Since August 30, 2021, I am assigned to investigate Violent Crimes Against Children (VCAC), which includes numerous federal, state, and local law enforcement agencies conducting proactive and reactive investigations involving online child exploitation. As a Special Agent, I am authorized to investigate violations of federal laws and to execute warrants issued under the authority of the United States. Specifically, as a Special Agent assigned as the Case Agent of a VCAC investigation, I investigate criminal violations related to online sexual exploitation of children. I have received on-the-job training in

the areas of child sexual exploitation including, but not limited to, possession, distribution, receipt, and production of child pornography, and interstate travel with intent to engage in criminal sexual activity, by speaking with and learning from other Special Agents assigned to the Bedford RA, and learning from and speaking with online undercover employees who work VCAC investigations. I have also participated in numerous search warrant operations and interviews supporting VCAC investigations while assigned to the Bedford RA.

4. Over the course of this investigation, I have conferred with other investigators who have conducted numerous investigations and executed numerous search and arrest warrants which involved child exploitation and/or child pornography offenses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. The facts set forth in this affidavit are based in part on my personal knowledge, information obtained during my participation in this investigation, information from others, including law enforcement officers, my review of documents and computer records related to this investigation, publicly-available information regarding Kik services, and information gained through my training and experience. I have set forth only the facts that I believe are necessary to establish probable cause that the SUBJECT ACCOUNT has been used to violate 2252A(a)(2) and 2252(a)(4)(B). There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes, as further described in Attachment B.

STATUTORY AUTHORITY

5. This application is part of an investigation into a Kik user with the username "Evangeliant" for the alleged distribution and possession of visual depictions of minors engaging in sexually explicit conduct (child pornography). Title 18, United States Code, § 2252A(a)(2) prohibits a person from knowingly distributing any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. Title 18, United States Code, § 2252(a)(4)(B) prohibits a person from knowingly possessing any child pornography that has been mailed, or using any means or facility of

interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711(3) and 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

BACKGROUND ON KIK SERVICES

7. Through training and experience, as well as Kik's guide for law enforcement and publicly available information, I know that Kik Messenger is a free social-networking service owned by MediaLab, Inc., which is headquartered in Santa Monica, California. Through the Kik Messenger application, Kik users can share text messages and other content, including videos and images. Kik users can create groups for communication or sending pictures and videos; they can also exchange private messages, photographs, and videos directly with individual Kik users. Kik users and groups are identified on the Kik app by whatever username and/or screen name they choose.

8. The Kik application is primarily used on mobile or "smart" devices, such as an Apple iPhone, Android cell phone, Apple iPad, or Android tablet. Although Kik is a platform for mobile devices, there are ways that it can be used on desktop or laptop computers. In order to do so, a person would have to install on the computer what is known as an "emulator," a program that emulates a mobile device environment.

9. Kik allows users to create a profile using a name and an email address. The email address is not verified by Kik. Additionally, Kik does not require a phone number for registration. While on Kik, Kik users can only see other Kik members' display name, username, and profile picture, which are all chosen by the Kik user.

10. Kik exchanges are called chats, whether they are conducted by text message or video. Kik Messenger allows for group chats with up to 50 participants. The platform also facilitates real-time video

chat options for live one-on-one video chat or private group video chats of up to six participants. Chats on Kik Messenger are not viewable remotely. Chats are only viewable through use of Kik user's password and on the device where the user has the application installed.

11. Kik messenger allows individuals to create public or private groups on their server which allows for multiple individuals to communicate and share files. Individuals within the group are also able to privately message other individuals within the group. The creator of the Kik group is called an owner. Through my training and experience, I know that the owner of a Kik group is either the individual who made the group or the longest active member after the original owner left the group. The owner of the group can make members of the group administrators which gives them the same privileges as the owner, such as adding individuals and removing them.

12. I am aware that Kik chats can be saved by the user in a variety of ways, including by taking screen shots using the mobile device on which Kik is used. However, once the screen shot has been created, it can easily be shared, saved, or transferred from the mobile device to any other electronic device through email, Bluetooth, or by saving the image to a removable SD card that can then be used to transfer the screen shot to the receiving device.

13. Kik collects information from and about users of the Kik Messenger application, including personally identifiable information, profile information, message content, conversation attributes, Kik communications, log and data usage information, device information, location information, and local storage information.

PROBABLE CAUSE

14. On August 19, 2020 a Philadelphia-based Online Covert Employee (OCE) was operating on Kik as an adult male when he joined a Kik group with the display name The group had no administrator noted, but the group owner was listed as .BobRoss. (Bobbie). The OCE watched activity within the group and engaged with members who were posting and trading Child Sexual Abuse Material (CSAM). On or about October 9, 2020 the OCE was promoted to the owner and administrator of #c.hild.p.orn. The OCE was promoted without any discussion on the topic. It is unknown how the OCE

became the owner/admin of the group. While the OCE was acting as the owner/admin, individuals sent CSAM directly to the OCE or were observed by the OCE posting CSAM to the group. During this time, Kik user and . group-member "Evangeliant" sent an image to the OCE of a prepubescent black female child, approximately 6-8 years old, in a bathroom with her legs spread exposing her vagina. The child is nude and seated on a toilet seat with her right leg is positioned on the back of the toilet.

15. On October 21, 2020 MediaLab responded to a subpoena for records related to the Kik user: "Evangeliant". An email account @yahoo.com and a first name of "Stark" were noted by Kik as being affiliated with the "Evangeliant" user profile.

16. On October 26, 2020, Oath Holdings, Inc. (the owner of Yahoo.com) responded to a subpoena for subscriber information associated with the email address @yahoo.com. The response indicated that the @yahoo.com account was created on January 13, 1997 and had since been terminated. Subscriber information associated with the @yahoo.com email account listed the city and state as Marlborough, New Hampshire, and an alternate email address of @top.monad.net. Public records show one ROBERT LEAHY, DOB: 1948 residing at

Marlborough, New Hampshire 03455.

17. On December 15, 2020, the Bedford RA opened an investigation. On August 30, 2021 SA Chambers was assigned as the Case Agent of the investigation.

18. During the period of October 15, 2021 through October 20, 2021 the OCE re-engaged in conversation with Kik user "Evangeliant". During the conversation, "Evangeliant" directed the OCE to the Kik group , which is also devoted to the exchange of child pornography. "Evangeliant" indicated that he was seeking images of preteen to teen black girls.

19. On October 19, 2021, "Evangeliant" provided the OCE two links to files stored on Mega, which I know to be a cloud-based, file-hosting service based out of New Zealand. One of the links (ending in "mbY1") was not valid. The second link, (ending in "12phQ") resolved to two folders which appear to contain depictions of minors engaged in sexually explicit conduct. The first folder, titled "sports," contained 93 files that appear to be, based on my training and experience, child pornography

images and videos. One of the child pornography videos located in the "sports" folder is titled "IMG_9407." The video is approximately 31 seconds in length and depicts a prepubescent female child, approximately 4-5 years of age, wearing a green shirt and pink underwear. The child is depicted laying on her back, and an adult male approaches her. Only the midsection/crotch area of the adult male is visible in the frame. The male unzips his pants, exposing his erect penis, which he then places in the child's mouth.

The second folder was named "young ebony" and contained 141 files, most of them videos. Many of the videos contain pornographic material depicting very young adult females and/or female teenagers of an indeterminate age, some of whom may be minors. Approximately twenty of the video files contain what appears to be, based on my training and experience, child pornography. One such video is titled " 334.mov" and depicts a female child, approximately 13 years of age, with no pubic hair and minimal breast development. At the beginning of the video, the child is clothed in only a black halter top, which she later removes. The child is lying on her back on a bed. An adult male is seen penetrating the child's vagina with his penis. Later in the video, the male places his penis in the child's mouth and she performs oral sex on him. The video is 8 minutes and 23 seconds in length.

20. On October 27, 2021 MediaLab responded to a second subpoena for records related to Kik user "Evangeliant". The records identified "Evangeliant" using a first name of: EVAN and an email address of: @yahoo.com. The email address is listed as "unconfirmed," which according to Kik means either the email address is invalid, or the user received a confirmation email from Kik but did not click on the link in the email to confirm the account. Also noted was the account appeared to use an Android Samsung phone.

21. Included with the Kik subpoena returns was a log of IP addresses used by "Evangeliant" to access the Kik account. The IP log shows numerous IP addresses that resolve to locations in Japan, the Czech Republic, and Los Angeles. This pattern of IP addresses may indicate "Evangeliant" is using a Virtual Private Network (VPN) to mask his online activity. A VPN conceals an internet user's geographic

location by connecting the user's device to another computer somewhere on the internet and allowing the user to browse the internet using that computer's internet connection.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

22. The evidence believed to be located within the Kik account is listed in Attachment B, which is incorporated by reference as if fully set forth herein, and is believed to be contained on servers and digital storage media maintained by and under the control of MediaLab, Inc., which owns and manages records for Kik. I request authority to search for and seize such material.

23. This application seeks a warrant to search all responsive records and information under the control of MediaLab, Inc., a provider subject to the jurisdiction of this court, regardless of where MediaLab has chosen to store such information[1]. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within MediaLab's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

24. Pursuant to 18 U.S.C. § 2703(g), this application and affidavit for a search warrant seeks authorization to require MediaLab and its agents and employees, to assist agents in the execution of this warrant. Once issued, the search warrant will be presented to MediaLab with direction that they identify the account described in Attachment A to this affidavit, as well as other subscriber and log records associated with the account, as set forth in Section I of Attachments B to this affidavit. The search warrant will direct MediaLab to create an exact copy of the specified account and records.

25. I, and/or other law enforcement personnel will thereafter review the copy of the electronically stored data and identify from among that content those items that come within the items identified in Section II to Attachments B for seizure.

---

[1] It is possible that MediaLab, Inc. stores some portion of the information sought outside of the United States. Under the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act"), the Stored Communications Act was amended to require that communications providers in the United States respond to legal process and return relevant data regardless of the location of the servers containing the data.

26. Analyzing the data contained in the forensic copy may require special technical skills, equipment, and software. It could also be very time-consuming. Searching by keywords, for example, can yield thousands of "hits," each of which must then be reviewed in context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. Keywords used originally need to be modified continuously, based on interim results. Certain file formats, moreover, do not lend themselves to keyword searches, as keywords, search text, and many common email, database and spreadsheet applications do not store data as searchable text. The data may be saved, instead, in proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases, as well. Consistent with the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. All forensic analysis of the data will employ only those search protocols and methodologies reasonably designed to identify and seize the items identified in Section II of Attachments B to the warrant.

27. Based on my experience and training, and the experience and training of other agents with whom I have communicated, it is necessary to review and seize a variety of Kik messages and documents that identify any users of the SUBJECT ACCOUNT and messages sent or received in temporal proximity to incriminating messages that provide context to the incriminating communications.

CONCLUSION

28. Based on the forgoing, I request that the Court issue the proposed search warrant authorizing a search of the SUBJECT ACCOUNT specified in Attachment A for the items more fully described in Attachment B.

Dated: December 8, 2021

Respectfully Submitted,

/s/ S. Vincent M. Chambers
S. Vincent M. Chambers
Special Agent
Federal Bureau of Investigation

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Honorable Andrea Johnstone
United States Magistrate Judge
District of New Hampshire
Dated: Dec 8, 2021

ATTACHMENT A

Property to Be Searched

This warrant applies to information related to and/or contained within the Kik account associated with the username "evangeliant", (the "SUBJECT ACCOUNT"), as well as information preserved from that account pursuant to a request made under 18 U.S.C. § 2703(f) that is stored at premises owned, maintained, controlled, or operated by MediaLab, Inc., a company based in Santa Monica, California.

Notwithstanding Title 18, United States Code, Section 2252A or similar statute or code, MediaLab shall disclose responsive data, if any, by delivering encrypted files to the United States Attorney's Office, District of New Hampshire, c/o AUSA Kasey Weiland, 53 Pleasant Street, 4th Floor, Concord, New Hampshire 03301 or by email Kasey.weiland2@usdoj.gov.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by MediaLab, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of MediaLab, Inc. (hereinafter "the Provider"), regardless of whether such information is stored, held or maintained inside or outside of the United States, including any messages, records, files, logs, or information that has been deleted but is still available to the Provider, or that has been preserved, the Provider is required to disclose the following information to the government for the SUBJECT ACCOUNT listed in Attachment A, from account creation through present:

a. All basic subscriber information including, but not limited to:

1. Kik username;
2. Email address, birthdate, and IP address used to register the account;
3. Current email address;
4. Phone number;
5. Device related information;
6. Display name;
7. Link to most current profile picture or background;
8. Kik account creation date and IP address; and
9. Timestamp and IP address of account logins and logouts;

b. All IP addresses associated with the SUBJECT ACCOUNT;

c. All transactional chat logs associated with the SUBJECT ACCOUNT;

d. Images and videos associated with the SUBJECT ACCOUNT including unknown usernames and IP address associated with the sender/recipients of the images and videos;

e. A date-stamped log showing the usernames that the SUBJECT ACCOUNT added and/or blocked from accounts;

f. All abuse reports associated to the SUBJECT ACCOUNT including unknown usernames;

g. All messages and emails sent to or from the SUBJECT ACCOUNT;

h. Any information relating to groups the SUBJECT ACCOUNT belonged to from account creation to present, including but not limited to:

1. Group create log including the creator's username and IP address;
2. Group join logs including the inviter and invitee usernames and IO addresses;
3. Group leave logs including the remover and removed username(s) and IP addresses;
4. Group transactional chat logs including senders IP addresses;
5. Images and videos sent to the group including the sender's and receiver's usernames, and IP address associated to the sender of the images and videos; and
6. Abuse reports including all usernames;

i. Account identifiers (e.g., usernames) and basic subscriber information for any accounts that are linked to or otherwise associated with the SUBJECT ACCOUNT (e.g., a separate user account registered using the same email address as the SUBJECT ACCOUNT);

j. All privacy settings and other account settings, including for individual Kik posts and activities;

k. All records pertaining to communications between Kik and any person regarding the user or the user's Kik account, including contacts with support services and records of actions taken.

MediaLab is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 8 U.S.C. § 2252(a)(2) (distribution of child pornography), 18 U.S.C. § 2252(a)(4)(B) (possession of child pornography) those violations found in the SUBJECT ACCOUNTe listed on Attachment A, including the following:

a. Information constituting evidence of production, distribution, storage, or solicitation of sexually explicit images or videos of minors;

b. Information constituting evidence of chat threads of a sexual nature relating to minors between the SUBJECT ACCOUNT and other Kik users;

c. Information constituting evidence indicating how, when, and by whom the Kik accounts were accessed or used to determine the chronological and geographic context of account access, use, and events relating to the crimes under investigation and to the identity of the Kik account owner;

d. Information constituting evidence indicating the Kik account owner's state of mind as it relates to the crimes under investigation;

e. Information constituting evidence of the identity of the person(s) who created or used the Kik accounts, including records that help reveal the whereabouts of such person(s); and

f. Information constituting evidence of the identity of any person(s) who communicated with the Kik accounts about matters relating to the crimes under investigation.